

## **Introduction – Malicious Website Verification**

Following this procedure will determine if a website is actually malicious or being used for malicious purpose(s). Based on this analysis, determine if an incident has possibly occurred and begin the next appropriate procedure.

### **Instructions**

**A.** Use these selected URL reputation tools below, to investigate what our security partners, other vendors, and other companies have discovered about the site. These URL reputation tools will identify:

- The category of the URL and if it has deemed malicious.
- Detection and analysis of web-based malware.
- Analyze files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners

\*\*\*If an URL is a shortening service provider e.g. tinyURL, goo.gl url, bitly, owly, or other TLD service provider:

- Expand shortened url first, and proceed with the rest of the work instruction.  
(Example of url expander service site; <http://urlex.org/>)



- <https://fortiguard.com/webfilter>

\*The category of the URL and if it's deemed malicious



- <https://virustotal.com> or <https://urlquery.net> or <https://urlscan.io>
- \*Detection and analysis of web-based malware
- \*Analyze files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners

urlquery.net is a service for detecting and analyzing web-based malware. It provides detailed information about the activities a browser does while visiting a site and presents the information for further analysis.

[Learn about the advanced settings](#)

Profile URL:

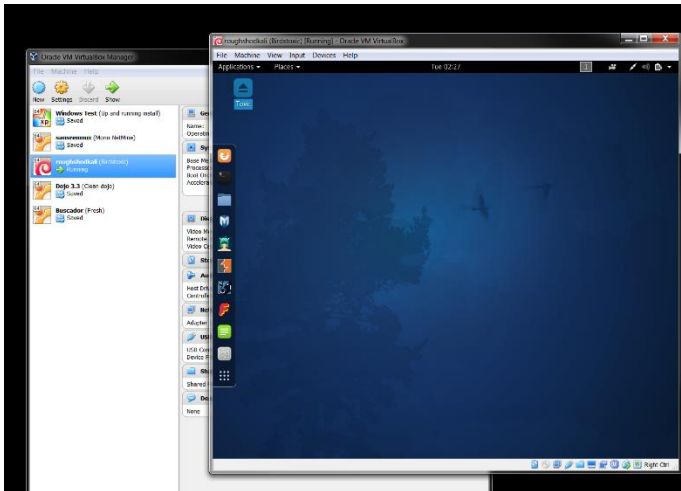


Analyze suspicious files and URLs to detect types of malware including viruses, worms, and trojans.

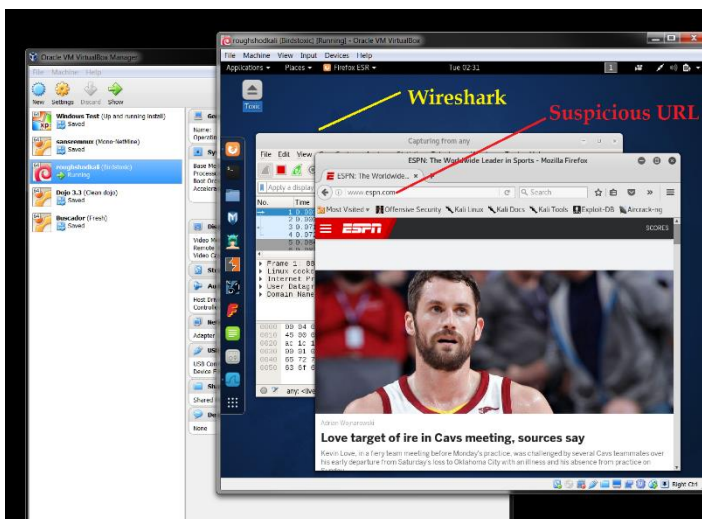
A blue square icon with a white document symbol and a blue circular arrow, indicating a file upload action.

By using VirusTotal you consent to our [Terms of Service](#) and [Privacy Policy](#) and allow us to share your submission with the security community. [Learn more](#)

- B.** Utilize a virtual machine, a dirty laptop connected to the outside internet line, or AWS ec2 instance to visit the URL in question and analyze the URL.
- Load a clean snapshot of Window or Linux to a virtual machine



- Start a network packet capture e.g. tcpdump / wireshark
- Visit the URL in question



- After 1 minute stop packet capture and examine the packet capture data and/or save packet capture files to be uploaded to static analysis site

```

2429 42.651922103 198.70.66.170 10.0.2.15 HTTP 3298 HTTP/1.1 200 OK (application/
2466 42.657316402 198.70.66.170 10.0.2.15 HTTP 10262 HTTP/1.1 200 OK (application/
2480 42.65954618 198.70.66.170 10.0.2.15 HTTP 682 HTTP/1.1 200 OK (text/css)
2522 42.696138468 198.70.66.170 10.0.2.15 HTTP 30917 HTTP/1.1 200 OK (text/css)
2550 42.725559965 23.36.32.88 10.0.2.15 HTTP 1284 HTTP/1.1 200 OK (text/javascr
2561 45.893297130 198.70.66.171 10.0.2.15 HTTP 3257 HTTP/1.1 200 OK (application/
2707 47.264671862 52.84.124.173 10.0.2.15 HTTP 288 HTTP/1.1 302 Moved Temporarily
2790 47.842064587 172.28.94.36 10.0.2.15 HTTP 921 HTTP/1.0 200 OK (GIF87a)
2807 47.860411391 198.70.66.178 10.0.2.15 HTTP 4653 HTTP/1.1 200 OK (application/
2809 47.862967638 50.17.164.80 10.0.2.15 HTTP 759 HTTP/1.1 302 Found
2858 47.961692553 139.104.188.6 10.0.2.15 HTTP 303 HTTP/1.1 200 OK (application/
2860 47.962969508 50.17.164.80 10.0.2.15 HTTP 288 HTTP/1.1 200 OK (application/
2885 48.072274863 172.82.206.19 10.0.2.15 HTTP 636 HTTP/1.1 200 OK (application/
2891 48.112654824 50.17.164.80 10.0.2.15 HTTP 993 HTTP/1.1 200 OK (application/
2898 48.134525572 198.70.66.178 10.0.2.15 HTTP 527 HTTP/1.1 200 OK (PNG)
2904 48.138606448 198.70.66.178 10.0.2.15 HTTP 1384 HTTP/1.1 200 OK (PNG)
2907 48.245737890 198.70.66.178 10.0.2.15 HTTP 1138 HTTP/1.1 200 OK (PNG)

Frame 180: 455 bytes on wire (3640 bits), 455 bytes captured (3640 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 104.154.170.133, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 52390, Seq: 1, Ack: 281, Len: 399
Hypertext Transfer Protocol
  HTTP/2.1 301 Moved Permanently
    Server: nginx
    Date: Tue, 23 Jan 2018 07:31:14 GMT
    Content-Type: text/html
    Location: https://purple.com/
    X-Type: default
    Content-Length: 178
    Age: 40
    Via: 1.1 localhost:localhost
  [HTTP response 1/1]
  [Time since request: 0.13260625 seconds]
  [Request in frame: 178]
  File Data: 178 bytes

```

- Print and reload the browser's developer tools to refresh the screenshot.

Time	Type	URL
10:41:01	script	http://techcrunch.com/{inline_script}
10:41:01	-- script	http://stats.wp.com/w.js?46
10:41:01	-- script	https://s2.wp.com/_static/??-eJyVjcsKwjAQRX/IdPqwiy7Eb0nToZnYjCEzafh
10:41:01	-- script	http://platform.twitter.com/widgets.js?ver=20111117
10:41:01	-- script	https://s1.wp.com/wp-content/js/devicepx.js?m=1429298047g
10:41:01	-- script	https://s2.wp.com/wp-content/mu-plugins/gravatar-hovercards/wpgroh
10:41:01	-- script	http://0.gravatar.com/js/gprofiles.js?ver=201520x
10:41:01	-- script	http://o.aolcdn.com/os_merge?file=/aol/beacon.min.js&file=/aol/omnitu
10:41:01	-- script	https://s1.wp.com/_static/??-eJyNkOsKwjAMhV/Irruhv8Rn2Wq2pFym3RD
10:41:01	-- script	http://stats.wp.com/w.js?46
10:41:01	-- script	https://s2.wp.com/_static/??-eJyVjcsKwjAQRX/IdPqwiy7Eb0nToZnYjCEzafh
10:41:01	-- script	http://platform.twitter.com/widgets.js?ver=20111117
10:41:01	-- script	https://s1.wp.com/wp-content/js/devicepx.js?m=1429298047g
10:41:01	-- script	https://s2.wp.com/wp-content/mu-plugins/gravatar-hovercards/wpgroh
10:41:01	-- script	http://0.gravatar.com/js/gprofiles.js?ver=201520x
10:41:01	image	https://s0.wp.com/wp-content/themes/vip/techcrunch-2013/assets/imag
10:41:01	image	https://s0.wp.com/wp-content/themes/vip/techcrunch-2013/assets/imag
10:41:01	image	https://s0.wp.com/wp-content/themes/vip/techcrunch-2013/assets/imag

## Checklist – Malicious URL Verification

- Is domain categorized as a known: Phishing, Malicious Websites, Newly Observed Domain, Newly Registered Domain, Spam URLs, Dynamic DNS – hosted site.
- Was suspicious website traffic associated with a known good domain.
- Was suspicious website traffic seen.
- Was suspicious traffic isolated.
- Was there any malware downloaded.
- Was there any redirects or callouts to foreign host(s)

Based on the analysis determine if an incident has possibly occurred and begin the appropriate procedure.